What is claimed is:

1. A method of designing a password-based authentication and key exchange protocol using a zero-knowledge interactive proof, comprising:

a first step of setting various kinds of system parameters required for authentication;

a second step of a user selecting a certain random number (r, x) in conformity with the set parameters, and sending to a server a message including a user ID, a test number (A=OWF(r)) to which a one-way function (OWF) is applied, and a first question number generation value X known only to the server and the user;

a third step of the server sending to the user a message including an authentication Auth of whether the server possesses a public key, and a second question number generation value Y known only to the server and the user;

a fourth step of the user authenticating the server by verifying the authentication Auth, computing a resultant value c of a secret coin tossing known only to the server and the user and a session key SK in a general zero-knowledge proof, and sending to the server a witness number B for user authentication; and

a fifth step of the server that stores a password verifier (V=OWF(f(P)) for the respective user verifying the witness number B using the test number A, the password verifier V, and the value c, and exchanging the session key SK by computing the session key SK.

2. The method as claimed in claim 1, wherein the witness number B is sent to the server using the value c, the random number r, and its own password P.

3. The method as claimed in claim 1, wherein the user authenticates the server by confirming whether the server possesses the password verifier.

4. The method as claimed in claim 1, wherein if the one-way function is based on an RSA problem, the password verifier is $V=[f(P)^{-1}]^e \bmod n$, where $n=p*q$(p and q are RSA fractions, e (fraction) is a public key, and f(P) is a function for expanding the password P into lg(n) bits.

5. The method as claimed in claim 1, wherein the witness number B is $B=r*f(P)^c \bmod n$, where $c=H(TSK||A)$, $TSK=H(K'||0)$, $K=[V^{-1}(X)]^y$, $K'=H(K||g^x||g^y||ID_{User}||ID_{Server}$, and H( ) is a hash function.

6. The method as claimed in claim 1, wherein authentication of the witness number B is performed using $B^e*V^c=A \bmod n$, where $c=H(TSK||A)$, $TSK=H(K'||0)$, $K=[V^{-1}(Y)]^x$, and $K'=H(K||g^x||g^y||ID_{User}||ID_{Server})$.

7. The method as claimed in claim 1, wherein if the one-way function is based on a discrete logarithm problem, the password verifier is $V=a^{-F(p)} \bmod p$, where a is a generator of Z^*_q, p is a fraction, and f(P) is a function for expanding the password P into lg(n) bits.

8. The method as claimed in claim 1, wherein the witness number is $B=r+f(P)*c \bmod q$, where $c=H(TSK||A)$, $TSK=H(K'||0)$, $K=[V^{-1}(X)]^y$, $K'=H(K||g^x||g^y||ID_{User}||ID_{Server}$, and H( ) is a hash function.

9. The method as claimed in claim 8, wherein authentication of the witness number B is performed using $a^BV^c=A \bmod p$, where $c=H(TSK||A)$, $TSK=H(K'||0)$, $K=[V^{-1}(Y)]^x$, and $K'=H(K||g^x||g^y||ID_{User}||ID_{Server})$.

10. The method as claimed in claim 1, wherein if the one-way function is based on a prime factorization problem, the password verifier is $[V_1=[f(P+1)^{-1}]^2 \bmod n$, $V_2=[f(P+2)^{-1}]^2 \bmod n$, $V_3=[f(P+3)^{-1}]^2 \bmod n$, ..., $V_k=[f(P+k)^{-1}]^2 \bmod n$, $V=H(V_1,V_2, ...,V_k)]$, where $n=p*q$(p and q are RSA fractions), and f(P) is a function for expanding the password P into lg(n) bits.

11. The method as claimed in claim 1, wherein the witness number is

$$B = r * \prod_{i=1,k} f(P+i)^{c_i}$$

where $c=H(TSK||A)$, $TSK=H(K'||0)$, $K=[V^{-1}(X)]^y$, $K'=H(K||g^x||g^y||ID_{User}||ID_{Server}$, and H( ) is a hash function.

12. The method as claimed in claim 11, wherein authentication of the witness number B is performed using

$$A = B^2 * \prod V_i^{c_i} \bmod n$$

where $c=H(TSK||A)$, $TSK=H(K'||0)$, $K=[V^{-1}(Y)]^x$, $K'=H(K||g^x||g^y||ID_{User}||ID_{Server}$, and c_i is an i-th bit.

13. The method as claimed in claim 1, wherein the server makes a random challenge transmitted for authentication from the server to the user known only to the server and the user to defend against an offline dictionary attack.